14812

Karsh & Co.
A Professional LLC
Certified Public Accountants
Cherry Creek Plaza II • 650 South Cherry Street, Suite 500
Denver, Colorado 80246-1803
(303) 825-1000 FAX (303) 825-8800

March 20, 2019

Dear Client:

For over 50 years, Karsh & Co. has been a trusted advisor for our clients. We are sincerely appreciative of your business and look forward to many more years of working together. We have always taken the issue of privacy seriously, and as part of that commitment, we are reaching out to you because we have become aware of data security incident that we discovered on February 28, 2019 involving the personal information of our clients.

We also wanted to thank you for your patience and understanding in this matter. Several of the clients who have become victims to this attack have reached out to offer their assistance to our investigative efforts, and their input has been invaluable.

We have engaged nationally recognized cybersecurity experts to assist us in our investigation and are working with the IRS to minimize potential impacts to our clients. We and have also reported this incident to the FBI and local law enforcement authorities.

While we are still working to learn what we can about these events, we wanted to tell you what we know so far and about steps you may be able to take to further protect yourself. Along with our efforts to minimize or eliminate potential harm, we encourage you to take preventive measures now to help prevent and detect any misuse of your information. **If you have not done so already, we strongly recommend you consider placing a credit freeze on your credit files**—please see more about this under "What you can do," below.

We are also offering all affected individuals a free one-year enrollment in a LifeLock identity theft protection and credit monitoring service. Please also read the enclosures for more information on how to activate your membership; the deadline to enroll is May 14, 2019. Please note that you must login to configure your settings after registration to ensure you will obtain the full benefits from this service.

Our clients' information is our first priority. Again we thank you for your understanding and cooperation as we work to investigate this incident and minimize the impact it will have on you. If you have any questions, again, please do not hesitate to reach out.

Sincerely,

Karsh & Co.
A Professional LLC

Ryan K. Petersen

Ryan K. Petersen
Certified Public Accountant

IMPORTANT INFORMATION – PLEASE READ CAREFULLY

1. What happened?

On or around February 28 we learned of an incident involving unauthorized access to the personal information of some of our clients. We are continuing to investigate the nature of the incident, and are notifying you because we believe it is possible that some of your personal information could have been accessed.

2. What information was involved?

To the best of the information we currently have, we believe that first and last names and social security numbers may have been obtained. Other personal information that could have been obtained includes the following: street address, email address, financial account information, date of birth, payroll information, and/or other information that Karsh held about individuals. The personal information accessed, if any, may vary by individual.

3. What we are doing

We immediately initiated an extensive investigation and have enlisted cybersecurity forensics specialists to assess the incident and to prevent or mitigate harms that could come from the unauthorized access. We have verified that all of our networks are secure and have taken measures to further ensure that your personal information is not vulnerable to any unauthorized access. Our experts are continuing to investigate and we will keep affected clients apprised as new information becomes available.

In addition, we have reported this matter to the appropriate government authorities. We have reached out to the IRS to notify them of the incident and to solicit their assistance with our investigation, and to law enforcement, including local police and the FBI, to obtain their assistance as well. We are also working with our clients and with the IRS to prevent further fraud, including by filing paper returns with the Form 14039 (Identity Theft Affidavit) as appropriate.

4. What you can do

1) ***Consider Filing a Police Report.*** You may want to file a police report, especially if you find suspicious activity on your credit reports or have reason to believe your information is being misused. Keep a copy of the police report as you may need it for your records.

2) ***Place a Credit Freeze.*** We strongly recommend you consider placing a credit freeze on your credit files. A freeze prevents an authorized person from using your personal identifying information to open new accounts or borrow money in your name. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. *See* https://www.identitytheft.gov/Steps for more information ("Consider adding an extended fraud

alert or credit freeze."). There are no fees for placing a credit freeze, though the agency may request you provide a police report or other type of incident report. *See more about this below.*

3) ***Monitor Account Statements and Credit Reports***. Check your account statements and credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. You may obtain a free credit report from each of the major credit reporting agencies by calling 1-877-322-8228 or by logging onto www.annualcreditreport.com. When you receive your credit reports review them for:
   a) accounts you did not open,
   b) inquiries from creditors you did not initiate,
   c) personal information that is not accurate, etc.
   If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

4) You can obtain more information from the Federal Trade Commission (FTC) and the credit reporting agencies about fraud alerts and security freezes. You can also initiate a credit freeze by contacting the reporting agencies – please see below:

Federal Trade Commission (FTC):

You can visit the FTC's Identity Theft website at https://www.identitytheft.gov/assistant to find helpful information for consumers who are victims of identity theft. Select the option for "Someone else filed a Federal Return using my information."

You may wish to file a complaint with the FTC at www.ftc.gov.

Phone: 1-877-ID-THEFT (1-877-438-4338).

Address: 600 Pennsylvania Avenue, NW
Washington, DC 20580

Credit reporting agencies:

TransUnion	Experian	Equifax
1-800-680-7289 www.transunion.com; P.O. Box 1000 Chester, PA 19022	1-888-EXPERIAN www.experian.com or www.experian.com/freeze.com P.O. Box 2104 Allen, TX 75013-0949	1-888-298-0045 www.equifax.com or www.freeze.equifax.com P.O. Box 740241 Atlanta, GA 30374-0241

PLEASE NOTE: By law, placing a credit freeze is free with all three agencies, but you may be asked to verify your identity and to provide information about this event and/or yourself such as your social security number and address history. You may also be asked to provide proof of your identification and mailing address by sending copies of documents such as your driver's license, social security card, pay stub or tax document, utility bill, or lease.

5. What else you should do

1) You should promptly **change your password(s) and security question or answer(s),** as applicable, for any Karsh platforms.

2) You should also take other steps to protect any **other online accounts** for which you use the same username or e-mail address and password and/or security question(s) and answer(s).

3) Prepare and submit a **Form 14039** to alert the IRS about the potential issue: https://www.irs.gov/pub/irs-pdf/f14039.pdf. **We can assist you with this form.**

4) If you are contacted by phone by anyone claiming to be a representative of the IRS, **do not give out any personal information**. Many incoming phone solicitations are scams.

5) You may receive a letter from the IRS requesting additional information. **If you receive a letter**:

   a) Respond immediately to the IRS via the phone number provided in the letter.

   b) Send us a copy of the notice, particularly if you would like us to correspond with IRS to process your tax return.

   c) Note that you may need a copy of your prior-year tax return, if you filed one, to help verify your identity.

   d) Visit https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works to learn more.

6) Register for an Identity Protection PIN ("IP PIN") if you are eligible.

   a) https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. **Note:** not all taxpayers are eligible for the program: See this link for more information: https://www.irs.gov/individuals/secure-access-how-to-register-for-certain-online-self-help-tools.